Abstract (Basic): JP 11175474 A

NOVELTY - A password management apparatus maintains login ID and user password . During effective login condition, a thyme password previously generated along with unique security code, is included in the HTML page of user service, generated dynamically. During next access, when the thyme password is detected to be effective, accessing of corresponding function of web server is approved.

USE - For authenticating user to access web servers in internet

ADVANTAGE - Enables maintenance of data without including any document in management directory of web server. Prevents inaccurate usage of web server, reliably.

Dwg.1/1

Title Terms: USER; AUTHENTICITY; SYSTEM; CONTROL; ACCESS; WEB; SERVE; ACCESS; CORRESPOND; FUNCTION; WEB; SERVE; THYME; PASSWORD; DYNAMIC; GENERATE; PAGE; USER; SERVICE; DETECT; EFFECT

Derwent Class: T01

International Patent Class (Main): G06F-015/00

File Segment: EPI

Manual Codes (EPI/S-X): T01-J

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（A）**　(11)特許出願公開番号

特開平11－175474

(43)公開日　平成11年(1999)７月２日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ

審査請求　未請求　請求項の数５　書面　（全　４　頁）

(21)出願番号　特願平9－369746

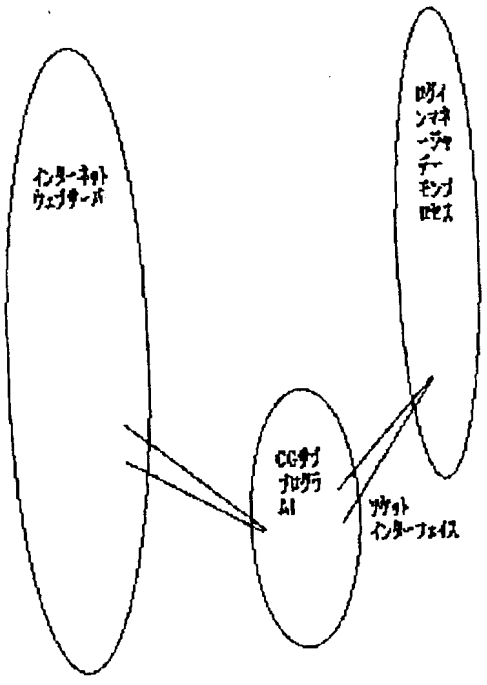
(22)出願日　平成９年(1997)12月10日

(71)出願人　393020889
マシンコントロールシステム有限会社
東京都品川区西大井４丁目21番10号

(72)発明者　田中　雅男
東京都品川区西大井４丁目21番10号

(54)【発明の名称】　ウェブサーバ用ログインマネージャ

(57)【要約】
【課題】ウェブサーバの不正使用を防止するセキュリティ管理と課金管理をすることが可能なログイン技術を提供する。
【解決手段】ユニークなセキュリティコードを発生するワンタイムパスワード発生装置と、ログインＩＤとユーザパスワードを管理するパスワード管理装置と、前記変換されたワンタイムパスワードとを連携づけ、有効なログイン状態である場合に前記ワンタイムパスワードに対応する機能の実行を許可するセキュリティ管理処理部とをウェブサーバのコンピュータ本体に備えるものである。



【特許請求の範囲】
【請求項１】ウェブサーバのログインにおいて、ユニークなセキュリティコードを発生するワンタイムパスワード発生装置とログインＩＤとユーザパスワードを管理するパスワード管理装置と、前記変換されたワンタイムパスワードとを連携づけ、有効なログイン状態である場合に、前記ワンタイムパスワードを動的に生成するユーザサービスのＨＴＭＬページ中に埋め込み、次回のアクセス時に、有効なワンタイムパスワードであるかどうかを検査することにより、ログイン状態の維持を管理する機能をコンピュータ本体にそなえる装置である。
【請求項２】ウェブサーバ用ログインマネージャ装置において、ログイン以後は、各ページのアクセスは、毎回ワンタイムパスワードにより、ユーザ認証されるため、その認証されたページ処理の課金情報ログを残し、その課金情報ログをもとに、定期的に、課金集計し、ウェブサーバシステムにおいて、アクセスページ単位の課金請求を実現する装置である。
【請求項３】請求項１の装置を実現する方式。
【請求項４】請求項２の装置を実現する方式。
【請求項５】ウェブサーバ用ログインマネージャ装置において、ログイン以後は、各ページのアクセスは、毎回ワンタイムパスワードにより、ユーザ認証されるため、ウェブサーバの管理ドキュメントディレクトリ外に置かれたコンテンツを動的にウェブサーバの管理ドキュメントディレクトリ内に転送して、コンテンツの配布管理を実現する装置である。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本技術は、ウェブサーバのセキュリティをワンタイムパスワードに応じてウェブサーバが管理する特定の機能の実行を許可するコンピュータ不正使用防止装置に適用して有効な技術に関するものである。
【０００２】
【従来の技術】近年、インターネットのウェブサーバを使用した業務が増加するにつれて、ユーザに関する課金や重複ログインに関して、ウェブサーバで管理したい状況になっている。
【０００３】従来のウェブサーバに蓄積されたデータの内、コンピュータの利用者の利用資格を確認し、コンピュータの不正使用を防止するユーザ認証には、パスワードを使用するベーシック認証が一般的である。
【０００４】前記ベーシック認証を使用する方法は、利用者を識別するユーザＩＤと利用者本人しか知ることができないパスワードをウェブサーバが管理しているＵＲＬ配下のディレクトリに対して、アクセスする許可をＵＲＬ単位に認証している。
【０００５】前記ウェブサーバとウェブブラウザの通信は、ＨＴＴＰ通信プロトコルによる、コネクションレスプロトコルを利用する方法である。
【０００６】
【発明が解決しようとする課題】前記従来技術を検討した結果、以下の問題点を見い出した。
【０００７】前記ベーシック認証でＵＲＬを認証する方法では、時系列的に見た場合、ある人のログイン処理をコンピュータがおこなっている時に、同一人物、あるいは別人が同じパスワードを使いログインした場合、後者のログイン認証の重複検査ができない。そのため、ユーザごとに検索履歴などの個人情報を壊す可能性があり、ある時間軸の中で、同一ＩＤに対して、多重ログインを阻止したいが、ベーシック認証ではできない。
【０００８】前記ＨＴＴＰ通信プロトコルは、コネクションレスプロトコルのため、ログイン後のページからアクションされ、動的に生成されたページからさらにアクションをしていくような同一ログインで時間的連続性を保証するような要求を処理するためには、動的に作成されたページ中にログインした個人を識別するなんらかの識別子を埋め込む必要がある。しかし、ログインＩＤやユーザのパスワードは、識別子にはなるが、これは個人の機密情報であるため、再利用される可能性のあるページ中にユーザパスワードを入れることはできない。
【０００９】動的に作成されたページがどのユーザがログインし生成したかを保証することにより、生成したページ単位に課金処理をおこないたい要求がある。
【００１０】本技術の目的は、コンピュータの不正使用を防止するセキュリティ管理の操作性を向上する事が可能な技術を提供することにある。
【００１１】本技術の他の目的は、ログイン後にそのユーザが動的に生成するページにセキュリティの確保されたワンタイムパスワードを埋め込むことにより、個人の機密情報であるユーザパスワードを隠蔽し、かつコンピュータ側ではログイン後のユーザを識別できる技術を提供することにある。
【００１２】本技術の他の目的は、静的なコンテンツをウェブサーバの管理外ディレクトリに置き、コンテンツ配布プログラムを経由して、動的にコンテンツを配布するコンテンツ配布管理ができる技術を提供することにある。
【００１３】本技術の他の目的は、ログイン後にそのユーザが静的あるいは動的に生成するページのアクセスにおいて決められた単価で課金する従量課金システムの技術を提供することにある。
【００１４】
【課題を解決するための手段】本技術によって開示される発明のうち、代表的なもののを説明すれば、下記のとおりである。
【００１５】（１）ウェブサーバのログインにおいて、ユニークなセキュリティコードを発生するワンタイムパスワード発生装置とログインＩＤとユーザパスワードを

管理するパスワード管理装置と、前記変換されたワンタイムパスワードとを連携づけ、有効なログイン状態である場合に、前記ワンタイムパスワードを動的に生成するユーザサービスのＨＴＭＬページ中に埋め込み、次回のアクセス時に、有効なワンタイムパスワードであるかどうかを検査することにより、ログイン状態の維持を管理する機能をコンピュータ本体にそなえる装置である。

【００１６】（２）前記（１）に記載されたウェブサーバ用ログインマネージャ装置において、ログイン以後は、各ページのアクセスは、毎回ワンタイムパスワードにより、ユーザ認証されるため、その認証されたページ処理の課金情報ログを残し、その課金情報ログをもとに、定期的に、課金集計し、ウェブサーバシステムにおいて、アクセスページ単位の課金請求を実現する装置である。

【００１７】（３）前記（１）に記載されたウェブサーバ用ログインマネージャ装置において、ログイン以後は、各ページのアクセスは、毎回ワンタイムパスワードにより、ユーザ認証されるため、ウェブサーバの管理ドキュメントディレクトリ外に置かれたコンテンツを動的にウェブサーバの管理ドキュメントディレクトリ内に転送して、コンテンツの配布管理を実現する装置である。

【００１８】

【実施例】（実施形態１）以下、本発明のウェブサーバ用ログインマネージャについて説明する。

【００１９】図１は、本実施形態のウェブサーバ用ログインマネージャの概略構成を示す図である。

【００２０】本ウェブサーバ利用者は、まず本システム利用に先立ち、サービス事務局より、利用資格として、ユーザＩＤとパスワードを発行してもらうことが必要です。

【００２１】サービス事務局より発行するユーザＩＤとパスワードは、ログインマネージャのパスワード管理処理部に登録します。

【００２２】利用者は、サービス事務局より発行されたユーザＩＤとパスワードを使いログインページのＵＲＬから、ログインマネージャのＣＧＩ処理部に入ってきます。

【００２３】このＣＧＩ処理部は、ログインマネージャデーモンプロセスとソケット通信を行い、ログインプロトコルでログインの要求を送ります。

【００２４】ログインマネージャデーモンは、送られてきたユーザＩＤとパスワードが、パスワード管理処理部に登録されているかをデータベースをサーチして確認します。

【００２５】パスワード管理処理の結果登録ユーザである場合は、ワンタイムパスワード発行処理部でワンタイムパスワードを発生させて、ユーザＩＤとワンタイムパスワードを関連づけ、ログインマネージャデーモンプロセスで、管理するアクティブリストに登録し、アクティブリスト監視タイマーで定期検査します。

【００２６】その結果を呼びだしたプロセスに通知し、登録ユーザであれば、ログインマネージャデーモンプロセスから渡されたワンタイムパスワードを保持しながら、ＣＧＩ処理部のページ処理機能を実行して、実際の利用者へのサービスを提供し、そのサービスの結果である利用者へ返すページにワンタイムパスワードのみをＨＴＭＬのヒドン属性に埋め込んで返します。

【００２７】また、このＣＧＩ処理部で、アクセスログと課金ログを保存して、以後のアクセス集計管理とユーザ毎の課金請求処理データになります。

【００２８】また、このＣＧＩ処理部で、ウェブサーバの外側に置かれた静的なコンテンツをウェブサーバの管理するドキュメントディレクトリにコピーし、配布を管理する機能も処理可能である。

【００２９】登録ユーザでない場合は、ログインエラー処理で利用者に通知。

【００３０】ワンタイムパスワードの埋め込まれた動的処理用のページから呼び出されるＣＧＩ処理部は、ワンタイムパスワードを、ログインマネージャデーモンプロセスに通信することにより、アクティブリストにワンタイムパスワードが登録されているかどうかを検査して、結果をＣＧＩ処理部へ返します。

【００３１】ウェブサーバから起動される、ＣＧＩサブプログラムは、ワンタイムパスワードを利用したログインマネージャデーモンからのセッション検査機能により、どのページからのアクセスが、どの利用者からのページであるかをログインマネージャデーモンからの結果をもとに判断し、ワンタイムパスワードによるウェブサーバから発生するページ毎にユーザ認証する方式の装置です。

【００３２】（実施形態２）以下、本発明のウェブサーバ用ログインマネージャの課金処理機能について説明する。実施形態１の中で、個人認証されたページ単位の課金ログ情報を定期的（月末処理）に集計することで、各ユーザＩＤ単位で、アクセスページとそのページ処理単価で、課金集計プログラムで処理することで、従量課金などの細かな請求処理データを作成することが可能である。

【００３３】

【作用および効果】本願において開示される発明のうち代表的なものよって得られる効果を簡単に説明すれば、下記のとおりである。

【００３４】（１）ウェブサーバのログインにおいて、１個人が１時期において、多重にログインする排他制御が可能になるため、１個人ごとのアクセス履歴を残す事が可能である。

【００３５】（２）ページアクセスの毎に、ユーザ認証が取れているため、課金すべきページに対して、従量課金をすることが、可能である。

【００３６】（３）静的なドキュメントでも、動的にコンテンツを配布することが可能になるため、ウェブサーバの管理ディレクトリにドキュメントを置かずに、データを保持することが可能なため、コンテンツ配布用プログラムを経由せずには、ウェブサーバからアクセスできないため、コンテンツを動的に管理することが可能になる。

【図面の簡単な説明】

【図１】本実施形態の概略構成図

【図１】